# Ensuring patient privacy in image data sharing for clinical research

Aryanto, Kadek Yota Ernanda

# Chapter 1
# **General introduction**

Clinical data sharing, including image data, between health enterprises has brought huge improvements in patient care [1]. It brings accurate and timely manner of large amount of data transfer that lead to best health diagnostics, treatments and decision making. While in research area, data sharing can also improve the accuracy of the research itself and also provide information regarding the risk or possibility of improvements of current methods use within the enterprises.

Data transmission utilizes the interoperability between various systems and standards since clinical data may come in different formats. The Digital Imaging and Communication in Medicine (DICOM) standard [2] has been commonly used for storing, viewing, and transmitting information in medical imaging [3]. It was developed to enable the exchange of data between different manufacturers and data sharing between institutions or enterprises. Its structure can be easily adapted and upgraded to accommodate changes in medical imaging technology [4].

## 1.1 Regulation, Rules, and The Tools

A DICOM file consists of viewable image and a header contains large variety of metadata elements which includes the identifiable information about the patient, study, and institution. These kinds of data are vulnerable to a breach that may be caused by organizational or systemic threat [5], by internal or external agents, intentionally or not. Therefore, sharing such sensitive data demands proper protection to ensure data safety and maintain patient privacy as required by the regulations.

In European Union (EU), patient data privacy and security are guaranteed by the Data Protection Directive 95/46/EC of 1995 that obligate the EU member states (countries) to protect the privacy of personal information that is processed within the member state regions [6]. To do the task many tools have been developed [7-17]. Each tool provides its own advantages in removing or replacing one or a selection of DICOM header elements. However, DICOM toolkits should be used with care when de-identifying sensitive data since they have a high risk of disclosing personal health information, especially when using the default configuration.

The most common methods used to de-identify such information are anonymisation and pseudonymisation, where the first method removes information carried by header elements or replaces the information with random data while the second one is done by replacing the most identifying fields within a data record using one or more artificial identifiers. Anonymisation caused the

remaining information cannot be used to reveal the patient identity at all and therefore claimed to be the most secure approach to ensure the privacy of DICOM data since it fully uncouples the data from the original patient [3]. Meanwhile, pseudonymisation still can be used by authorized personnel to track down the real identity of the patient which most frequently used in clinical analysis, processing, and research [18][19][20].

## 1.2 Implementation

Correct and timely migration of the data from the current to the new Picture Archiving and Communication System (PACS) is one of the key success factors of the PACS transition. On the other hand, it also become one of the major concerns [21] and often underestimated [22]. The whole migration process should be prepared carefully and thoroughly investigated with regards to required time, manpower and equipment resources [21]. Therefore, it is a challenging process that involves many stakeholders.

PACS has evolved from predominantly radiological service into the fundament of the image management system utilized throughout the entire healthcare enterprise for clinical practice and research [23-26]. Therefore, other than just the ease-of-use of the systems introduced to handle a certain task, the ease of integration of those systems have also become an important issue to adequately fulfill the requirements of smooth integration into the daily work processes. A system that provides fast and easy integration profiles to normal workflow with support of imaging data de-identification is important in facilitating data distribution within a hospital environment. Multiple channels for de-identification processes enable the system to provide multi tasks to be done within one time and become a major advantage in both clinical practice and clinical research setting. Web technology helps the built system to have a wider access and therefore will also make further integration possible. However, once more, going beyond the borders of the own institution would require proper protection of the patient personal data and privacy.

Compared to the physical film, the use of portable media to distribute patient data give beneficial in term of cost and the loss of studies so therefore it is claimed to be able to improve the patient care [27,28]. However, distribution through portable media may also hampers the evaluation of the image data where data are vulnerable to alteration and unsafe for a sensitive data distribution [29]. A system that that incorporates the study data from the CDs into the normal hospital workflow using a decentralized upload of the CD data [30] is important. However,

the need for storage of external data is vastly growing at considerable costs and will require a better approach to the CD handling in combination with installation and acceptation of network based sharing using XDS between hospital enterprises.

To perform safe, secure and standardized clinical data sharing in a network of trusted partners, the Cross-Enterprise Document Sharing (XDS) profile [31] was initiated as one of the Integrating the Healthcare Enterprise (IHE) [32] profiles. Later, a content profile to extend the XDS profile was developed, known as the Cross-Enterprises Document Sharing for Imaging (XDS-I) profile [33], to describe how the image and report data are shared between health enterprises. However, when employed in a research setting, the implementation of XDS-I introduces the challenge of providing convenient and easy access to the shared study-related data from other enterprises without compromising patient privacy and patient data confidentiality.

## 1.3 Thesis Outline

This thesis describes the studies regarding the rules and regulations within the European Union (EU) about patient data privacy and provides design and implementations of infrastructures for image data sharing in the health enterprises to meet the requirement of those regulations. **Chapter 2** describes the development of image storages and distribution in the radiology environment in the last two decades. **Chapter 3** describes the regulations regarding data protection in the EU. Numerous tools were built and developed to provide the efforts of ensuring patient data protection. However, serious problems related to the patient privacy may rise when users do not make a careful selection for the tool they use. The comparison of various de-identification toolkits are studied in **chapter 4**. **Chapter 5** discusses the migration methodology from one PACS to another, together with possible problems and challenges that can occur during the process. **Chapter 6** provides the institutional image data distribution system which utilizes the Clinical Trial Processor (CTP) tools developed by the RSNA. **Chapter 7** describes the pitfall and consequences from the usage of portable media in data sharing with decentralized upload of DICOM data into PACS. **Chapter 8** explains how a de-identification toolkit can be implemented to the hospital normal workflow. In **chapter 9**, methodologies for image de-identification within the XDS environment are described.

## References

[1] Adler-Milstein, J, Jha, A.K, "Sharing Clinical Data Electronically A Critical Challenge for Fixing the Health Care System", Journal of American Medical Association, 307(16):1695-1696

[2] N. E. M. A. (NEMA), "The DICOM Standard." [Online]. Available: http://medical.nema.org/.

[3] O. Pianykh, "What Is DICOM?," in in Digital Imaging and Communications in Medicine (DICOM), Springer Berlin Heidelberg, 2012, pp. 3–5.

[4] M. Mustra, K. Delac, and M. Grgic, Overview of the DICOM standard, vol. 1, no. September. IEEE, 2008, pp. 10–12.

[5] Appari, A; Johnson, M.E, Information security and privacy in healthcare: current state of research, Int. J. Internet and Enterprise Management, Vol. 6, No. 4, 2010

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of pe rsonal data and on the free movement of such data. Document "1995/281 1 EN JOL". Available via http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. Accessed February 2015.

[7] González DR, Carpenter T, van Hemert JI, Wardlaw (2010) J. An open source toolkit for medical imaging de-identification. DOI: 10.1007/s00330-010-1745-3

[8] RSNA, "CTP-The RSNA Clinical Trial Processor." [Online]. Available: http://mircwiki.rsna.org/index.php?title=CTP-The_RSNA_Clinical_Trial_Processor.

[9] D. Library, "DICOM Library - Anonymize, Share, View DICOM files ONLINE." [Online]. Available: http://www.dicomlibrary.com.

[10] Dicomworks project, "DicomWorks - Free DICOM software." [Online]. Available: http://www.dicomworks.com.

[11] DVTk, "DVTk Project." [Online]. Available: http://www.dvtk.org/.

[12] GDCM, "GDCM: Grassroots DICOM library." [Online]. Available: http://gdcm.sourceforge.net/wiki/index.php/Main_Page.

[13] Andreas Knopke, "K-Pacs." [Online]. Available: http://k-pacs.net/.

[14] P. Publishing, “PixelMed Java DICOM Toolkit.” [Online]. Available: http://www.pixelmed.com.

[15] C. de R. P. H. Tudor, “The Tudor Dicom Tools.” [Online]. Available: http://santec.tudor.lu/project/optimage/dicom/start.

[16] Masahiro YAKAMI, “YAKAMI DICOM Tools.” [Online]. Available: http://www.kuhp.kyoto-u.ac.jp/~diag_rad/intro/tech/dicom_tools.html.

[17] Lakhani, P, Chen, J, Nagy, P, Safdar, N, “Protecting Your Patient's Privacy: Is Your DICOM Anonymizer Working for You?”, Radiological Society of North America 2009 Scientific Assembly and Annual Meeting, November 29 - December 4, 2009 ,Chicago IL.http://archive.rsna.org/2009/8011488.html Accessed September 10, 2014

[18] R. Noumeir, A. Lemay, and J.-M. Lina, “Pseudonymization of Radiology Data for Research Purposes,” Journal of Digital Imaging, vol. 20, no. 3, pp. 284–295, 2007.

[19] T. Neubauer and B. Riedl, “Improving patients privacy with Pseudonymization.,” Studies In Health Technology And Informatics, vol. 136, pp. 691–696, 2008.

[20] T. Neubauer and J. Heurix, “A methodology for the pseudonymization of medical data.,” International journal of medical informatics, vol. 80, no. 3, pp. 190–204, Mar. 2011.

[21] Jung H, Kim H-J, Kang W-S, et al. Migration of Medical Image Data Archived Using Mini-PACS to Full-PACS. J Digit Imaging 2004;17(2):100-108.

[22] Maass M, Kosonen M, Kormano M. Radiological Image Data Migration – Practical Experience and Comparison of the Costs of Work. Acta Radiologica 2001;42:426-429.

[23] Huang HK (2003) Enterprise PACS and image distribution. Comput Med Imaging Graph 27:241–253. DOI: 10.1016/S0895-6111(02)00078-2

[24] Rajala T, Savio S, Penttinen J, et al (2011) Development of a research dedicated archival system (TARAS) in a university hospital. J Digit Imaging 24(5): 864-73. DOI: 10.1007/s10278-010-9350-1

[25] Bandon D, Lovis C, Geissbühler A, Vallée JP (2005) Enterprise-wide PACS: Beyond Radiology, an Architecture to Manage All Medical Images. Acad Radiol. 12(8):1000-9. DOI: 10.1016/j.acra.2005.03.075

[26] van de Wetering R, Batenburg R, Oudkerk M, van Ooijen PMA, Brinkkemper S, Scheper W. (2011) A Situational Alignment Framework for PACS. J Digit Imaging. 24(6): 979-992. DOI: 10.1007/s10278-011-9368-z.

[27] Flanders AE (2009) Medical image and data sharing: are we there yet? Radiographics 29(5):1247-51. DOI: 10.1148/rg.295095151

[28] Mehta A, Dreyer K, Thrall J (1999) Enhancing availability of the electronic image record for patients and caregivers during follow-up care. Journal of Digital Imaging 12(Suppl 1): 78–80. DOI: 10.1007/BF03168762

[29] McEvoy FJ, Svalastoga E. (2009) Security of patient and study data associated with DICOM images when transferred using compact disc media. Journal of Digital Imaging 22(1): 65-70. DOI: 10.1007/s10278-007-9068-x

[30] P. M. A. Van Ooijen, J. Guignot, G. Mevel, and M. Oudkerk (2005) Incorporating out-patient data from CD-R into the local PACS using DICOM worklist features. Journal of Digital Imaging. DOI: 10.1007/s10278-005-5158-9

[31] P. Seifert, "Cross-Enterprise Document Sharing," 2011, 2011. [Online]. Available: http://wiki.ihe.net/index.php?title=Cross_Enterprise_Document_Sharing.

[32] "Cross-enterprise Document Sharing for Imaging." [Online]. Available: http://www.ihe.net.

[33] R. Noumeir, "IHE cross-enterprise document sharing for imaging: design challenges," in Proc. SPIE 6145, Medical Imaging 2006: PACS and Imaging Informatics, 2006.